

**Trustworthy Computing
Academic Advisory Board**

July 30 – 31 2003

Agenda

- Introduction of Participants
- Administrative Details
 - Contacts - Dave Ladd x30404, Noelle Triou, x25575
 - Travel update
 - Videotaping
 - Confidentiality
- First Session - Status:
 - Progress on action items from last meeting
 - Introduction of Peter Cullen (New Privacy Officer)
 - Update on GeCAD acquisition
 - Update on Pelican acquisition
 - Update on Steve Lipner's changing role
 - Update on MSR management changes
 - Discussion of outstanding board slots
 - Discussion of latest critical bug fixes, processes, etc.
- Second Session - Threat Modeling 10:00am - 3:30pm
- Final Session - Windows Privacy Standard 4:00pm - 6:00pm
- Dinner - 7:00pm

Action Items

Procedural Commentary

• Speaker Quality/Presentation Type

- Need to have senior leadership present for the entire meeting, so these people can get first-hand understanding of credibility of current technical staff and approach (Senior people from presenting org need to be present in addition to Microsoft corporate management)

DONE - ONGOING

• Timing/length of discussion/format

- More and longer breaks
- Two day meeting is okay, but fewer talks day two
- First session should be for committee discussion
- Have speakers be available at dinner reception
- There was not enough time for informal discussions with speakers, following their talks
- Longer board only session for summary needed

DONE

DONE

DONE

DONE

DONE

DONE

• Other items

- Create an email alias for the board members
- We should get copies of slides after the meeting
- We should get copies of minutes after the meeting
- We should get copies of a to-do list based on topics raised in the meeting
- Better read ahead package would be preferred
- Prefer to hear about things when we can still have impact
- Board should have the opportunity to have input on the agenda
- We may want to change the composition of the board

DONE - Listserv

DONE - WEBSITE

DONE - WEBSITE

DONE - Action List

PARTIALLY DONE

PARTIALLY DONE

DONE - Action List

OUTSTANDING

Action Items

Technical Commentary

• **STRIDE/Windows Security Push/Software Engineering Process**

- Need to better understand the threat model, STRIDE, etc., and to understand the extent to which management and real programmers understand the virtues and limits of attack surfaces, etc. **DONE - THIS SESSION**
- What is the whole software development process? In particular, design and architecture is part of the process and we need to see how security and privacy concerns come into play here. **FUTURE SESSION**
- Revisit the security push process vis a vis long term culture change. **OPEN QUESTION**
- Bring in MS technical education to hear their views on how teachable this stuff is. **FUTURE SESSION**
 - Revisit the extent to which training and security push is becoming pervasive in the corp.
- Assurance: How does Microsoft measure whether security is increasing/improving? **OPEN QUESTION**

• **Longhorn**

- There are lots of parts of Longhorn to discuss. Two obvious ones: **FUTURE SESSION**
 - New authorization architecture
 - Reboot discussion

• **Privacy**

- How to "operationalize" the privacy policy. Can it be handled like a threat analysis? **THIS SESSION**
- How do technical and legal policies and cultures interact? **FUTURE SESSION**
 - Test case: privacy in Palladium?

SD³ At Work – MS03-007

Windows Server 2003 Unaffected



~~IF I HADN'T HAD
IT I WOULD HAVE BEEN VULNERABLE~~

Code made more conservative during Security Push

~~Even if I was vulnerable~~

IIS 6.0 not running by default on
Windows Server 2003

~~Even if I was running~~

IIS 6.0 doesn't have WebDAV enabled by default

~~Even if I did have
WebDAV enabled~~

Minimum buffer length for POST is 65536 by default
(>64kb needed)

~~Even if it wasn't the
right enough~~

Process fails rather than executes malicious code,
due to buffer overrun detection code (GS)

~~Even if there was an
exploitable buffer overrun~~

Would have occurred in `inetd.exe` which is now
running as 'network service'

SD³ At Work – MS03-007

Windows Server 2003 Unaffected



THE ~~NTFS~~ ~~FILE~~ ~~SYSTEM~~ ~~IS~~ ~~NOT~~ ~~VULNERABLE~~

Code made more conservative during Security Patch

Even if it was vulnerable

IIS 6.0 not running by default on Windows Server 2003

Even if it was running

IIS 6.0 doesn't have WebDAV enabled by default

Even if it did have WebDAV enabled

minimum 64kb buffer in IIS 6.0 is set by default (>64kb needed)

Even if the buffer was large enough

Process fails rather than executes malicious code, due to buffer overrun detection code (GS)

Even if there was an exploitable buffer overrun

Would have occurred in `wsnp.exe` which is now running as 'network service'

Action Items

Technical Commentary

• STRIDE/Windows Security Push/Software Engineering Process

- Need to better understand the threat model, STRIDE, etc., and to understand the extent to which management and real programmers understand the virtues and limits of attack surfaces, etc. **DONE - THIS SESSION**
- What is the whole software development process? In particular, design and architecture is part of the process and we need to see how security and privacy concerns come into play here. **FUTURE SESSION**
- Revisit the security push process vis a vis long term culture change. **OPEN QUESTION**
- Bring in MS technical education to hear their views on how teachable this stuff is. **FUTURE SESSION**
 - Revisit the extent to which training and security push is becoming pervasive in the corp.
- Assurance: How does Microsoft measure whether security is increasing/improving? **OPEN QUESTION**

• Longhorn

- There are lots of parts of Longhorn to discuss. Two obvious ones: **FUTURE SESSION**
 - New authorization architecture
 - Reboot discussion

• Privacy

- How to "operationalize" the privacy policy. Can it be handled like a threat analysis? **THIS SESSION**
- How do technical and legal policies and cultures interact? **FUTURE SESSION**
 - Test case: privacy in Palladium?